CYBER ATTACKS DURING

THE WAR ON TERRORISM:

A PREDICTIVE ANALYSIS

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES
AT DARTMOUTH COLLEGE

September 22, 2001

Michael A. Vatis
Director
45 Lyme Road
Hanover, NH 03755
603-646-0700

REPORT DOCUMENTATION PAGE

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 9/22/2001	3. REPORT TYPE AND DATES COVERED Report 9/22/2001

4. TITLE AND SUBTITLE
Cyber Attacks During the Ware on Terrorism: A Predictive Analysis

5. FUNDING NUMBERS

6. AUTHOR(S)
Michael A. Vatis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Institute for Security
Technology Studies
Dartmouth College
45 Lyme Road
Hanover, HN 03755

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 Words)*

This paper should be viewed as a clear warning to policymakers and security professionals. Just as the terrorist attacks of September 11, 2001 defied what many thought possible, cyber attacks could escalate in response to United States and allied retaliatory measures against the terrorists responsible for the attack. This paper examines case studies of political conflicts that have led to attacks on cyber systems, such as the recent clashes between India and Pakistan, Israel and the Palestinians, and NATO and Serbia in Kosovo, and the tensions between the U.S. and China over the collision between a Chinese fighter plane and an American surveillance plane.

14. SUBJECT TERMS
IATAC Collection, terrorism, cyber attacks, NATO

15. NUMBER OF PAGES
29

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED

NSN 7540-01-280-5500

THIS REPORT IS DEDICATED
TO
THE MEMORY OF JOHN O'NEILL.

John was a 31-year veteran of the FBI, who served most recently as a Special Agent in Charge in the New York field office, responsible for counterterrorism and counterintelligence matters. In that capacity, John oversaw the worldwide investigations into Osama bin Laden and the Al Qaeda organization, including the investigations of the 1998 bombings of the U.S. embassies in Kenya and Tanzania and the 2000 bombing of the USS Cole in Yemen. John retired from the FBI this past August and became the head of security at the World Trade Center in New York. John is missing and believed to have died in the terrorist attacks on the World Trade Center on September 11. John perished after going back into one of the burning towers to help victims and assist in the evacuation.

May the example set by John, and all of the first responder community who made the ultimate sacrifice to help others on September 11, 2001, inspire all of us to strengthen our resolve to eradicate terrorism in all its forms.

EXECUTIVE SUMMARY

This paper should be viewed as a clear warning to policymakers and security professionals. Just as the terrorist attacks of September 11, 2001 defied what many thought possible, cyber attacks could escalate in response to United States and allied retaliatory measures against the terrorists responsible for the attack. This paper examines case studies of political conflicts that have led to attacks on cyber systems, such as the recent clashes between India and Pakistan, Israel and the Palestinians, and NATO and Serbia in Kosovo, and the tensions between the U.S. and China over the collision between a Chinese fighter plane and an American surveillance plane.

LESSONS FROM RECENT CYBER ATTACK CASE STUDIES:

1. Cyber attacks immediately accompany physical attacks (Page 9)

2. Cyber attacks are increasing in volume, sophistication, and coordination (Page 9)

3. Cyber attackers are attracted to high-value targets (Page 9)

More importantly, the paper conducts a predictive analysis of the potential sources of attacks that could emerge in the wake of U.S. retaliation against the terrorists, the types of these attacks, and potential targets. When the United States and its allies launch their retaliatory action, there is a strong possibility of cyber attacks from hostile groups:

POTENTIAL SOURCES OF CYBER ATTACKS

- **Terrorist Groups** (Page 12)
- **Terrorist Sympathizers and Anti-U.S. Hackers** (Page 13)
- **Targeted Nation-States** (Page 12)
- **Thrill Seekers** (Page 14)

Based on factual analysis, we believe members of these groups will likely use cyber attack tools against the U.S. and allied states. Many of these tools are commonly available.

CYBER ATTACKERS DURING THE WAR ON TERRORISM ARE LIKELY TO:

1. Deface electronic information sites in the United States and allied countries and spread disinformation and propaganda. (Page 14)

2. Deny service to legitimate computer users in the U.S. and allied countries through denial of service attacks (DoS), the use of worms and viruses, and the exploitation of inherent computer security vulnerabilities. (Page 15)

3. Commit unauthorized intrusions into systems and networks belonging to the United States and allied countries, potentially resulting in critical infrastructure outages and corruption of vital data. (Page 17)

Finally, this study makes specific recommendations concerning how the United States and its allies could protect their information systems against the possible cyber onslaught. Several measures can be applied to ameliorate the threat of cyber attacks. Please refer to the sections referenced below for more detail:

CRITICAL CYBER SECURITY MEASURES DURING THE WAR ON TERRORISM:

1. Raise and maintain a heightened level of cyber alert and raising logging levels in times of acute crisis (Page 19)

2. Report of suspicious activity to law enforcement immediately to facilitate the warning and investigative processes (Page 19)

3. Apply and follow standard 'best practices' for computer and physical security; applying regular software updates, and installing worm protection, intrusion detection systems and firewalls (Page 19)

4. Secure critical information assets by implementing recommended measures against known exploits and back up all vital systems and information (Page 20)

5. Utilize ingress and egress filtering to protect against Distributed Denial of Service attacks (Page 20)

It is our hope that this product will highlight the increased threat of cyber attacks posed to the critical infrastructures of the United States and its allies and encourage further action towards securing our vital national assets.

CONTENTS

INTRODUCTION

The threat of terrorist attacks against U.S. citizens and U.S. interests around the world has become the Nation's most pressing national security issue. As of this writing, the United States is preparing its retaliation to the horrific terrorist attacks that took place on the morning of September 11, 2001. The campaign, if carried to the lengths necessary to eradicate the terrorist organization(s) responsible, will be fierce, protracted, and bloody. This is particularly true if the U.S. government follows through on its determination to go after nations that have supported the terrorist attacks.

American and allied military strikes are likely to lead to further terrorist strikes against American and allied citizens and interests, both in the U.S. and abroad. This aggression will likely take a variety of forms and may include cyber attacks by terrorist groups themselves or by targeted nation-states. Even more likely are cyber attacks by sympathizers of the terrorists, hackers[i] with general anti-U.S. or anti-allied sentiments, and thrill seekers lacking any particular political motivation. During the past five years, the world has witnessed a clear escalation in the number of politically motivated cyber attacks, often embroiling hackers from around the world in regional disputes.

In addition, the number, scope, and level of sophistication of cyber attacks unrelated to any political conflict are increasing rapidly. Where antecedent attacks were relatively benign, recent attacks have targeted vital communications and critical infrastructure systems. In the weeks and months to come, cyber attacks will evolve further, exposing vulnerabilities not yet identified by computer security experts. The recent Code Red and Nimda worms, for example, each exploited new vulnerabilities in Microsoft's IIS server software. In fact, we have already witnessed the first signs of cyber activity related to the terrorist attacks on September 11, 2001.[1]

The following four case studies provide relevant historical precedents that offer a starting point for analyzing the cyber activity we are likely to see in the near future.

---

[i] This study uses the term hacker to refer to and individual who illegally gains access to or enters another's information system. Footnote definitions were compiled from three sources in addition to ISTS scientists (cnet.com, sans.org, and techtarget.com).

FOUR CASE STUDIES: PHYSICAL CONFLICT AND CYBER ATTACKS

Afghanistan's Neighbors: The Pakistan/India Conflict

The tension between India and Pakistan over Kashmir, the disputed territory bordering both countries, is particularly salient due to its proximity to Afghanistan. This country is home to many of Al Qaeda's terrorist training camps and is likely to be a target of U.S. and allied retaliatory strikes. Sympathizers on both sides of the Kashmir conflict have used cyber tactics to disrupt each other's information systems and disseminate propaganda. Pro-Pakistan hackers eager to raise global awareness about the conflict have hit Indian sites especially hard.
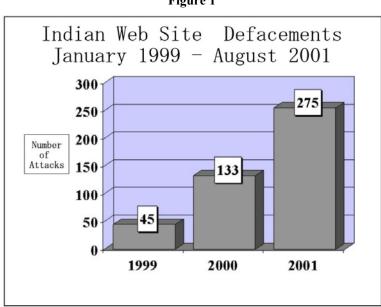
Figure 1

Indian Web Site Defacements
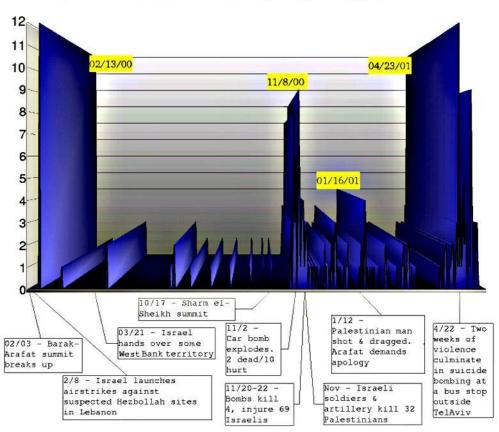January 1999 – August 2001

The number of pro-Pakistan defacements of Indian web sites has risen markedly over the past three years: 45 in 1999, 133 in 2000, and 275 by the end of August 2001 as illustrated in **Figure 1**.[2] Indian sites defaced by Pakistani hacker groups including G-Force and Doctor Nuker have been either political, highly visible, or involved in information dissemination (for example, the Indian Parliament, the TV network Zee, the Asian Age newspaper, the Indian Institute of Science, and the Bhabha Atomic Research Center.)[3] In the case of the Bhabha Atomic Research Center, five megabytes[ii] of possibly sensitive nuclear research or other information was reportedly downloaded.[4] Another pro-Pakistan hacker group, the Pakistan Hackerz Club, has also targeted U.S. sites in the past, defacing sites belonging to the Department of Energy and the U.S. Air Force.[5] This conflict illustrates the vulnerability of critical infrastructure systems to cyber attacks and the increasing willingness of groups to target sensitive systems during political conflicts.

[ii] Megabyte: a measure of computer data. A byte usually denotes 8 bits which the computer treats as a single unit. Although mega is Greek for a million, a megabyte actually contains 1,048,576 bytes.

The Israel/Palestinian Conflict

Paralleling the Middle East's most violent conflict, the ongoing cyber battle between Israelis and Palestinians has escalated over the past few years. **Figure 2** is a graphical representation of the web site defacement of Israeli computers mapped against political events in the region from late 1999 to early 2001. This comparison reveals a close connection between conflict in the physical and cyber worlds.

Figure 2

Israel (.il) Top-Level Domain
Website Defacements vs. Key Physical Events

Statistics on defacements to websites belonging to Israel's .il top-level domain (TLD) were retrieved from attrition.org. Each plot on the graph represents the daily total of new defacements reported. In no way are these numbers believed to be complete, but merely representative of relative activity across this period.[6]

This cycle of attack and counter-attack reveals the breadth of cyber targets, attack methodologies, and the vulnerability of electronic infrastructures. Cyber attackers have perpetrated significant web site defacements, engineered coordinated distributed denial of

service (DDoS)[iii] attacks and system penetrations[iv], and utilized worms[v] and Trojan horses[vi] in their efforts.

- ▪ The current bout of cyber attacks was spurred in part by the kidnapping of three Israeli soldiers on October 6, 2000. In response, pro-Israeli hackers launched sustained DDoS attacks against sites of the Palestinian Authority, as well as those of Hezbollah and Hamas.

- ▪ Pro-Palestinian hackers retaliated by taking down sites belonging to the Israeli Parliament (Knesset), the Israeli Defense Forces, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and others.[7]

- ▪ The Palestinian attacks, which have been dubbed a 'cyber jihad,' are following a strategy of phased escalation. According to one of the participating groups, UNITY: Phase 1 targeted Israeli government sites; Phase 2 directed attacks against Israeli economic services, such as the Bank of Israel; Phase 3 involved hitting the communications infrastructure, such as Israel's main Internet service provider (ISP)[vii] NetVision[8]; and Phase 4 calls for a further escalation, including foreign targets.

The Former Republic of Yugoslavia (FRY)/NATO Conflict in Kosovo

Cyber attacks were also directed against North Atlantic Treaty Organization (NATO) infrastructures as allied air strikes hit Former Republic of Yugoslavia (FRY) targets in Kosovo and Serbia during the spring of 2000. This event involving a nation-state and its regime's sympathizers provides insight into potential targets of groups hostile to the United States during the imminent U.S. and allied military retaliation to the September 2001 terrorist attacks

- ▪ During the bombing campaign, NATO web servers[viii] were subjected to sustained attacks by what NATO sources suspected to be hackers in the employ of the FRY military.[9] All of NATO's approximately 100 servers, hosting NATO's international website and e-mail traffic, were reportedly subjected to 'ping

---

[iii] Distributed Denial of Service attack (DDoS): action(s) by distributed computers that prevent any part of another computer system from functioning in accordance with its intended purpose.

[iv] System penetration: the successful unauthorized access to a computer system.

[v] Worm: an independent program that replicates itself from machine to machine across network connections. A worm often congests networks as it spreads.

[vi] Trojan horse: a program that appears legitimate but containing hidden code allowing unauthorized collection, exploitation, falsification, or destruction of data on a host computer.

[vii] Internet Service Provider (ISP): owners and providers of service over networks and computers on the Internet backbone (the lines that carry the majority of Internet information)

[viii] Web server: a system or program that provides network service such as disk storage or file transfer on the World Wide Web.

saturation'[ix] DDoS assaults and bombarded with thousands of e-mails, many containing damaging viruses[x].[10] The attacks periodically brought NATO servers to a standstill over a number of days.

- The communications attacks on NATO servers coincided with numerous website defacements of American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of the FRY government.[11]

- Although services directly related to coordinating and executing the bombing campaign are believed to have been unaffected, the attacks against NATO's communications infrastructure caused serious disruptions in both internal and external communications and services.[12]

U.S. – China Spy Plane Incident

The repercussions of the mid-air collision between an American surveillance plane and a Chinese fighter aircraft on April 1, 2001, also offer insight into how political tensions increasingly find expression in cyber attacks. The ensuing political conflict between the two major powers was accompanied by an online campaign of mutual cyber attacks and website defacements, with both sides receiving significant support from hackers around the globe.

Chinese hacker groups, such as the Honker Union of China and the Chinese Red Guest Network Security Technology Alliance, organized a massive and sustained week-long campaign of cyber attacks against American targets, which led the National Infrastructure Protection Center (NIPC) in the U.S. to issue an advisory on April 26, 2001, warning of "the potential for increased hacker activity directed at U.S. systems during the period of April 30, 2001 and May 7, 2001."[13] Chinese hackers used Internet postings and Internet Relay Chat (IRC)[xi] to plan and coordinate their assault against U.S. systems. Access to the chat rooms[xii] was restricted by the need for a username and password to gain access. It remains unclear whether the Chinese government sanctioned these attacks, but, in light of the fact that these activities were highly visible and no arrests were made by Chinese officials, it can be assumed that they were at least tolerated, if not directly supported by Chinese authorities.

After approximately 1,200 U.S. sites, including those belonging to the White House, the U.S. Air Force and the Department of Energy, had been subjected to DDoS attacks or defaced with pro-Chinese images, the attack was stopped. It should be noted that a

---

[ix] Ping saturation: Ping is an Internet program that verifies Internet protocol (IP). An IP address is a 32-bit number that identifies each sender or receiver of information that is sent across the Internet. Ping saturation is a denial of service attack method were a target computer is overwhelmed with ping requests keeping legitimate users from accessing data on the target system.

[x] Virus: a program that infects other programs by modifying them to include a copy of itself.

[xi] Internet Relay Chat (IRC): is a communications method for Internet users to exchange information in real time.

[xii] Chat room: a generic term used to describe chat areas or virtual spaces where users can communicate and exchange information in real time.

number of recent Internet worms including Lion, Adore, and Code Red are suspected of having originated in China.[14]

LESSONS FROM CYBER ATTACK CASE STUDIES

> **U.S. and allied military strikes may result in cyber attacks against American and allied information infrastructures with significant economic, political or symbolic value.**

Cyber Attacks Immediately Accompany Physical Attacks

The preceding case studies show a direct relationship between political conflicts and increased cyber attack activity. Further, they highlight that this malicious cyber activity can have concrete political and economic consequences. In the Israel/Palestinian conflict, following events such as car bombings and mortar shellings, there were increases in the number of cyber attacks. Subsequent to the April 1, 2001 mid-air collision between an American surveillance plane and a Chinese fighter aircraft, Chinese hacker groups immediately organized a massive and sustained week-long campaign of cyber attacks against American targets.

Politically Motivated Cyber Attacks Are Increasing in Volume, Sophistication, and Coordination

Indian top level domain web defacements attributed to pro-Pakistan attackers have increased from 45 to over 250 in just 3 years.[15] Approximately 1,200 U.S. sites, including those belonging to the White House and other government agencies, were subjected to DDoS attacks or defaced with pro-Chinese images over one week in 2001.[16] Volume increases have been compounded by increases in sophistication and coordination. The sustained cyber attack by Chinese hackers and the Israeli/Palestinian cyber conflict show a pattern of phased escalation. Former Republic of Yugoslavia and Serbian attackers repeatedly disrupted NATO's communications infrastructure. Critical analysis of the targets of Pakistani, Palestinian, and other malicious aggressors indicates new levels of peril for countries that do not harden their information infrastructures. As demonstrated in the case studies, expansive targeting strategies for disrupting communications and information infrastructures have been utilized in the past.

Cyber Attackers Are Attracted to High Value Targets

Electronic high value targets are networks[xiii], servers[xiv], or routers[xv], whose disruption would have symbolic, financial, political, or tactical consequences. Palestinian groups'

[xiii] Network: a series of points or nodes (computers) interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.

[xiv] Server: a computer that provides the information, files, and other services to users (client) computers.

assault on Israeli banking and financial institutions' web sites is a warning for potential attacks on the U.S. economy. The 'Code Red' worm targeted the White House web site, intending to disable a political symbol of the American government.

RELEVANT TRENDS IN CYBER ATTACKS

With regard to general trends in cyber attacks, including those with no apparent political motivation, the overall sophistication of computer attacks has been steadily increasing. Whether motivated by financial gain or simply the challenge of breaking through defenses, attackers have been gradually ratcheting up the quality of their attacks for years. Furthermore, the wide and rapid dissemination of new exploit 'scripts' has made it possible for even unsophisticated programmers to take advantage of these advanced techniques.

Worms

The terms virus and worm are often used synonymously to describe malicious, autonomous computer programs. Most contemporary computer viruses are in fact worms. The worm epidemic of recent months, enabled by a common 'buffer overflow'[xvi] exploit, illustrates this phenomenon. Buffer overflows allow attackers to hijack legitimate computer programs[xvii] for illicit purposes, and they were once the dominion of only the most elite programmers. In the past five years, however, buffer overflow attacks have become more and more popular, and they are now the favorite among hackers of all skill levels. In June 2001, a computer security company identified a weakness in a popular web server program that could lead to a buffer overflow exploit.[17] The company published a benign exploit to demonstrate its point, but within days of the initial report a malicious program exploiting the identified weakness was making the rounds in the hacker world. Less than a month later, the Code Red worm appeared, leveraging the same weakness to spread itself to other machines running the web server software. Several weeks later, the Code Red II worm was created, employing the same mechanism but this time leaving behind a back door[xviii] that would allow any hacker to gain control of the infected machine. Recently, the Nimda worm appeared using a combination of Code Red's implanted back door and other weaknesses to maximize its record-setting propagation.

[xv] Router: a device that determines the next network point to which a packet should be forwarded toward its destination. A packet is the unit of data that is routed between an origin and a destination on the Internet

[xvi] Buffer overflow: an event in which more data is put into a buffer (computer data holding area) than the buffer has been allocated. This is a result of a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back doors leading to unauthorized system access.

[xvii] Program or software: in computing, a program is a specific set of ordered operations for a computer to perform.

[xviii] Back Door: a hole in the security of a computer system deliberately left in place by designers or maintainers or established by maliciously manipulating a computer system.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks have also evolved over time. DDoS attacks employ armies of 'zombie'[xix] machines taken over and controlled by a single master to overwhelm the resources of victims with floods of packets[xx]. These attacks are best known in the context of the high-profile attacks of February 2000, where popular e-commerce web sites were shut down by simultaneous attacks. Since that time, the popularity of high-speed home Internet access (via cable modems[xxi] and DSL[xxii]) has increased, and the commanders of DDoS zombie armies are taking advantage of this popularity. Preying on the lax security of the average home computer user, attackers have found ways to plant malicious programs to give themselves remote control of home computers. Many of these machines are now unwitting participants in DDoS attacks.[18]

Unauthorized Intrusions

Unauthorized computer intrusions[xxiii] and the loss of sensitive information are of great concern to businesses and governments alike. The theft of money or credit card numbers, proprietary information, or sensitive government information can have devastating consequences. Although there was a time when intrusions were limited to curious hackers, organized crime and other organized groups eventually realized the benefits of collecting poorly protected electronic information for financial or other gain. In March 2001, the NIPC issued a warning that organized crime had made significant inroads in cyberspace.[19] A series of intrusions, collectively known as Moonlight Maze, in U.S. government systems over a period of several years may have originated in Russia. The first attacks were detected in March 1998 and, in the course of this sustained assault, hundreds of unclassified networks used by the Pentagon, the Department of Energy, NASA, as well as a variety of defense contractors, may have been compromised. While authorities insist that no classified systems were breached, it is undisputed that vast quantities of technical defense research were illegally downloaded. In one case, a Hewlett Packard printer at the Navy's Space and Naval Warfare Systems Command Center (SPAWAR) in San Diego was reportedly reprogrammed to print out additional copies of all documents to a printer in Russia.[20]

[xix] Zombie: an insecure server compromised by a hacker who places software on it that, when triggered, will launch an overwhelming number of requests toward an attacked web site. Generally used in coordination with other zombies machines.

[xx] Packet: the unit of data that is routed between an origin and a destination on the Internet.

[xxi] Modem: a device that modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device.

[xxii] DSL: (Digital Subscriber Line) is a technology for bringing high-bandwidth information over conventional copper twisted pair telephone lines. Bandwidth (the width of a band of electromagnetic frequencies) is used to measure (1) how fast data flows on a given transmission path, and (2) the width of the range of frequencies that an electronic signal occupies on a given transmission medium. All digital and analog signals have a bandwidth.

[xxiii] Intrusion: any set of actions that attempt to compromise the integrity, confidentiality or availability of a computer resource.

Cyber attackers in response to U.S. and allied military strikes during the war on terrorism could employ any number of sophisticated attack tools and techniques to disrupt or compromise critical infrastructure systems. Exploits and attack tools are becoming ever more sophisticated; supporting the possibility that cyberterrorism may take a quantum leap in this conflict.

POTENTIAL GEOPOLITICAL SOURCES OF ATTACK

The U.S. and allied retaliatory military action against those responsible for planning and executing the terrorist actions on September 11, 2001 may result in cyber attacks against the United States. The potential attackers are grouped in four categories: terrorists, targeted nation-states, terrorist sympathizers or those with general anti-U.S. or anti-allied sentiments, and thrill seekers who may not be politically motivated, but are merely seeking notoriety.

Terrorist Groups

It is unclear whether Osama bin Laden's international Al Qaeda organization or other terrorist groups have developed cyber warfare capabilities, or how extensive these capabilities may be. To date, few terrorist groups have used cyber attacks as a weapon. However, terrorists are known to be extensively using information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely.[21] For instance, the convicted terrorist, Ramzi Yousef, who was responsible for planning the first World Trade Center bombing in 1993, had details of future terrorist plots (including the planned bombing of 12 airliners in the Pacific) stored on encrypted[xxiv] files on his laptop computer. At the same time, the September 11, 2001 attacks on the World Trade Center and Pentagon and previous terrorist targets such as the British security forces discovery that the Irish Republican Army (IRA) planned to destroy power stations around London, demonstrate an increasing desire by terrorist groups to attack critical infrastructure targets. The World Trade Center attacks not only took lives and property but closed markets and destroyed a significant component of the financial information infrastructure in New York City. Thus, trends seem clearly to point to the possibility of terrorists using information technology as a weapon against critical infrastructure targets.

Targeted Nation-States

Several nation-states, including not only Afghanistan, but also U.S.-designated supporters of terrorism, such as Syria, Iraq, Iran, Sudan and Libya[22], could possibly become the focus of U.S. military operations.[23] Perhaps most significantly, many foreign nations have identified the utility of developing cyber attack techniques for purposes of engaging in covert espionage against U.S. government networks or U.S. industry, or for employing information warfare'[xxv] against the U.S. [24] As the recent Defense Science Board report

---

[xxiv] Encryption: is the conversion of data into a form, called ciphertext that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

[xxv] Information warfare: actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending one's own information, information based processes, and information systems.

stated: "At some future time, the United States will be attacked, not by hackers, but by a sophisticated adversary using an effective array of information warfare tools and techniques."[25] Amongst the nations thought to be developing information warfare capabilities are Iraq and Libya, who could be targeted by U.S. and allied strikes as part of the war on terrorism. China, North Korea, Cuba, and Russia, among others, are also believed to be developing cyber warfare capabilities.[26]

Asymmetric warfare[xxvi] may be one of the few ways to compete against an adversary with overwhelming superiority in military and economic power. Countries with a developed cyber attack capability may employ information warfare against the United States and its allies if attacked. Further, the possibility exists that nation-states not directly involved in American retaliatory action could launch cyber attacks against U.S. systems under the guise of another country that is the focus of the war on terrorism. This is of particular concern as it is possible to disguise the origins of information attacks with relative ease.

Terrorist Sympathizers and Anti-U.S. Hackers

If historical trends continue, attacks by those sympathetic to the terrorist group(s) responsible for the September 11, 2001 attacks on the United States and those with general anti-U.S. and anti-allied sentiments are more likely than attacks by the terrorists themselves or by nation-states. If the American campaign against terrorism is perceived as a "crusade"[27] against people of the Muslim faith, the Middle East could become polarized into two camps. Muslim groups around the world could become players in this scenario, and many have significant experience in launching sophisticated and sustained cyber attacks. In this context, a variety of pro-Muslim hacker groups, such as G-Force Pakistan, The Pakistan Hackerz Club or Doktor Nuker, could utilize these tactics against the United States and its allies. As mentioned above, the Pakistan Hackerz Club has already launched attacks against U.S. targets in the past.

There is also a real danger that a wider polarization, involving groups with any form of grievance against the United States or its allies, could ensue, potentially creating a large and diverse hostile coalition. Such a coalition could encompass religious fanatics, anti-capitalists, those opposing the U.S. for its support of Israel, and Chinese hackers, among others.

The anti-capitalism and anti-globalization movement has employed violent tactics in recent years to demonstrate its opposition to the values that define the global status quo. Following the terrorist attacks of September 11, 2001, some anti-capitalism extremists applauded the action as a just reward for American imperialism.[28] These extremists and some moderate supporters of such movements could become involved in a concerted cyber campaign against the United States and its allies. Chinese hackers could also become involved in a cyber conflict because they may feel that they still have scores to settle with the United States. The recent online exchange between American and Chinese

---

[xxvi] Asymmetric warfare: the use of unconventional tactics to counter the overwhelming conventional military superiority of an adversary including conventional terrorism, classic guerrilla war and the use of weapons of mass destruction, but also such innovative approaches as cyber-attacks and information warfare.

hackers is still fresh in the memory of groups such as the 'Honker Union of China', which launched a weeklong campaign against American systems earlier this year. Further, many Chinese are still angry over NATO's accidental bombing of the Chinese embassy in Belgrade in 2000.

Thrill Seekers

Any conflict that plays out in cyberspace will invariably attract a huge number of hackers and script kiddies[xxvii] who simply want to gain notoriety through high profile attacks. This category of attackers may not be driven by political or ideological fervor, but simply the desire to achieve bragging rights about their exploits. Those just jumping on the bandwagon of a cyber conflict between the United States and its enemies pose a relatively low threat to American systems. The level of skill and sophistication of these attacks will probably be relatively low, due to the fact that these hackers often employ pre-fabricated hacker tools to launch attacks. Moreover, these thrill seekers are not highly motivated and could lose interest if the conflict drags on. However, the likelihood of attacks from thrill seekers is extremely high because of the intense media coverage of the situation. Thus, the possibility of gaining notoriety is enhanced.

Although this category of potential attackers may be seen as merely delivering nuisance attacks, the potential for critical systems to be knocked offline by these attackers at inopportune times remains. For example, DDoS attacks against prominent web sites in February 2000, such as those belonging to CNN and Yahoo!, and a number of recent computer worms or viruses, exhibited no evidence of political or financial motivation. Nonetheless, each had a significant economic impact and caused major disruptions.

POTENTIAL CYBER ATTACKS AND TARGETS DURING THE WAR ON TERRORISM

The final section of this paper identifies the potential types and targets of cyber attacks that we may see during the war on terrorism.

Web Defacements and Semantic Attacks

As the case studies portend, politically motivated web site defacements will likely continue to escalate as the war on terrorism is fought. Minor intrusions can result in defacements and anti-American or pro-terrorist propaganda. The most serious consequences of web defacements would involve 'semantic' attacks.[29] Such attacks entail changing the content of a web page subtly, thus disseminating false information. A

[xxvii] Script kiddie: a term used to describe individuals who break security on computer systems without understanding the exploit they are using. A specific example is a computer user who uses a Unicode attack by copying a line of text into their Internet browser window to attack a system. Unicode provides a standard for international character sets by assigning a unique number for each character. It is a compendium of commonly used character sets like ASCII, ANSI, ISO-8859 and others and may be used to change the appearance of an HTTP request while leaving it functional. HTTP (hypertext transfer protocol) is the protocol used to transmit and receive all data over the World Wide Web. A protocol is a set of communications rules that computer systems use. A Unicode attack allows attackers to disguise the payload used in an exploit and evade detection. The first major Unicode vulnerability was documented against Microsoft Internet Information Server (IIS) in October 2000.

semantic attack on a news site or government agency site, causing its web servers to provide false information at a critical juncture in the war on terrorism, could have a significant impact on the American population. Potential targets for web defacements and semantic hacks are any government or military web sites, high volume sites such as search engines, e-commerce sites, and news services.

Domain Name Service (DNS) Attacks

Computers connected to the Internet communicate with one another using numerical IP addresses. Domain name servers (DNS) are the 'Yellow Pages' that computers consult in order to obtain the mapping between the name of a system (or website) and the numerical address of that system. For example, when a user wants to connect to the CNN web site (cnn.com), the user's system queries a DNS server for the numerical address of the system on which the CNN web server runs (64.12.50.153). In this example, if the DNS server provided an incorrect numerical address for the CNN web site, the user's system would connect to the incorrect server. Making matters worse, this counterfeit connection would likely be completed without arousing the user's suspicion. The result would be that the user is presented a web page that he believes is on the CNN web server but, in reality, is on the attacker's server. An attacker could disseminate false information with a successful attack on a select DNS server (or group of servers), bypassing the need to break into the actual web servers themselves. Moreover, a DNS attack would prevent access to the original web site, depriving the site of traffic.

The system of domain name servers on the Internet is hierarchical. Local DNS servers maintain up-to-date, authoritative information about their own zones only and rely on communication with other DNS servers for information about remote zones. At the top of the hierarchy are root name servers that maintain authoritative information about which server is responsible for each local zone. Historically, successful DNS server attacks have been perpetrated against local DNS servers, causing traffic to selected sites to be redirected or lost. However, the potential exists for attacks on the root DNS servers, and the likelihood of an attack of this kind occurring may increase during the war on terrorism.

Distributed Denial of Service (DDoS) Attacks

Distributed denial of service (DDoS) attacks against high value targets (political and economic) are also likely to escalate during that war on terrorism since defending against these attacks is a formidable task. Hackers regularly launch DDoS attacks against an array of targets but the danger lies in a coordinated attack on significant national resources such as communications, banking, and financial targets. DDoS attacks against critical communication nodes would be particularly harmful, especially during a period of crisis. In the hours after the attacks in New York, when the phone circuits were overloaded, the Internet and its communication options, such as email and chat channels, were the only means for many people to communicate. Potential targets for DDoS attacks are chat and mail servers, government web sites, high volume sites such as search engines, e-commerce sites, and news services. As demonstrated in the Kosovo conflict, military web sites and communications systems are especially likely to receive DDoS attack variants.

Worms

The past six months have witnessed an unprecedented number of prolific 'worms' (e.g. Code Red, Ramen, Lion) some of which are suspected of having been created in response to political events. The vulnerabilities worms exploit are usually well known to systems administrators and able to be remedied, but often go un-patched on enough systems to cause major problems in the information infrastructure. Analysis by ISTS scientists of recent worm code, and discussion among experts in the computer security community of high profile worms, has resulted in the consensus that these intelligent software agents did not carry destructive payloads. A worm similar to Code Red could do much more serious damage with only minor design modifications. This analysis points to the conclusion that if maximum destruction is a hostile adversary's goal, worms are a cost effective way to significantly disrupt the United States' national information infrastructure. New worms may contain a sleep phase, in which the worm will infect as many hosts as possible, before activating its destructive payload perhaps in order to coordinate with a conventional terrorist attack.

Some researchers have predicted the emergence of new classes of worms (Warhol worms, flash worms)[30] which could spread in minutes or even seconds, leaving little or no time for system administrators to react. It is reasonable to expect that new variants of old worms will appear and be renamed to allude to the terror attacks in New York and Washington.[31]

Hybrid worms that combine a series of historically successful exploits to maximize effectiveness are certain to appear in the near future, if not during the war on terrorism.[32] Inevitably, there will be new worms based on vulnerabilities that are not yet known, and therefore, not immediately patchable. Worms employing such 'zero day exploits' could leave the custodians of information systems with no choice but to shut down services until patches are available, effectively resulting in a physical denial of service. Recent worms examined by computer security experts have been relatively crude in technological construction, perhaps aimed at easy targets to attract significant media attention. These worms may be used to shield more sophisticated and malicious worms, operating alongside their noisier cousins and targeting critical infrastructure systems.

Routing Vulnerabilities

Routers are the 'air traffic controllers' of the Internet, ensuring that information, in the form of packets, gets from source to destination. Routing operations have not yet seen deliberate disruption from malicious activity, but the lack of diversity in router operating systems leaves open the possibility for a massive routing attack. For example, the vast majority of routers on the Internet uses Cisco's Internetwork Operating System (IOS), and vulnerabilities in the Cisco IOS have been uncovered in recent months. While routers are less vulnerable than most computers due to the fact that they offer fewer services, there is the possibility that a current or as yet undiscovered vulnerability could be used to gain control of a number of backbone routers.

As the Melissa virus demonstrated in 1999, a lack of cyber diversity (i.e., the reliance on a single software or hardware product for certain functions) increases the chances of a simple but widely effective attack. If an attacker could find a common vulnerability, the

ensuing attack on routing operations would bring the Internet to a halt. One example is possibly attacking the border gateway protocol (BGP),[xxviii] which routers use to make decisions about where to send traffic on the Internet. This protocol is vulnerable to information poisoning that could corrupt routing tables. The result of this action would be a very effective Internet 'black hole' where large volumes of information headed for destinations all over the world would be lost.

Currently, the only authentication[xxix] mechanism for BGP updates is an optional encryption scheme named 'MD5 hashing'[xxx] that has not been widely adopted into use by router administrators. Internet backbone operators and service providers, who maintain the routers on which the Nation's information infrastructure depends, are not obliged to follow standards or regulations for maintaining security on routers. These operators must be particularly sensitive to any abnormal activity in routing behavior during the war on terrorism.

Infrastructure Attacks

Serious cyber attacks against infrastructures, through unauthorized intrusions, DDoS attacks, worms, or Trojan horse programs, or malicious insiders, have been the subject of speculation for several years.[33] Vulnerabilities in the Nation's power distribution grid were first exposed during the Joint Chiefs of Staff exercise "Eligible Receiver." Mr. Kenneth H. Bacon, Pentagon spokesperson, stated, "we did learn that computer hackers could have a dramatic impact on the nation's infrastructure, including the electrical power grid."[34] This vulnerability was exploited for real in June 2001, when computer hackers, routed through networks operated by China Telecom, penetrated the defenses of a practice network of the California Independent Systems Operator (Cal-ISO) for 17 days.[35] The specter of an unanticipated and massive attack on critical infrastructures that disables core functions such as telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services, has been raised in a number of reports on national security[36] and by the NIPC. The degrees to which these infrastructures are dependent on information systems, and interrelated to one another, are still not well understood. Neither is the extent to which these information systems are exposed to outside entry from the Internet.

[xxviii] Protocol: in information technology, the special set of rules that end points in a telecommunication connection use when they communicate.

[xxix] Authentication: the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords.

[xxx] Hashing: the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms. MD5 is a digital signature algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual.

Information systems associated with these critical infrastructures must be considered a likely target for terrorists, nation-states, and anti-U.S. hackers in the age of asymmetrical warfare. Some examples:

- **Banking and financial** institutions utilize infrastructures that are vulnerable to cyber attack due to their dependence on networks. However, this sector still operates largely private networks and intranets with very limited external access, thus affording it some protection from external cyber attack.

- **Voice communication systems** are vulnerable to proprietary software attacks from insiders familiar with the technical details of the system. This includes 911 and emergency services telephone exchanges.

- **Electrical infrastructures** have sensors that assist engineers in shutting down components of the national grid in times of natural disaster, which could become vulnerable to cyber manipulation, potentially resulting in power outages.

- **Water resources** and the management of water levels are often controlled by sensors and remote means. Physical security, in addition to heightened cyber security awareness, must be followed during the impending conflict.

- **Oil and gas** infrastructures widely rely on the use of computerized Supervisory Control and Data Acquisition (SCADA) and Energy Management Systems (EMS). These systems could be vulnerable to cyber attack with the potential of affecting numerous economic sectors, such as manufacturing and transportation.

Malicious insiders are the greatest threat to our critical national infrastructures. Insiders armed with specialized knowledge of systems and privileged access are capable of doing great harm. The tragedy of September 11, 2001 illustrates that terrorists live and operate within the United States, obtaining specialized skills with deadly intentions.

Compound Attacks

Individually, any one of the scenarios discussed here could have serious consequences. However, a multi-faceted attack employing some or all of the attack scenarios in compound fashion could be devastating if the United States and its allies are unprepared. A compound cyber attack by terrorists or nation-states could have disastrous effects on infrastructure systems, potentially resulting in human casualties. Such an attack could also be coordinated to coincide with physical terrorist attacks, in order to maximize the impact of both.

RECOMMENDATIONS

The Nation Must Be On High Cyber Alert During The War On Terrorism

System administrators and government officials in the U.S. and allied countries should be on high alert for the warning signs of impending hostile cyber activity, particularly during periods immediately following military strikes or covert operations. Reconnaissance by potential attackers is a fact of life in network operations, but changes in 'normal' scanning activity should be considered highly suspicious during this period and reported to the appropriate authorities listed in the related online resources appendix (Page 22) and incident reporting guidelines (Page 23). As an additional precaution, logging levels should be temporarily raised to trap as many events as possible to increase the fidelity of subsequent law enforcement and/or counterintelligence investigation, and enable the issuance of specific warnings by the NIPC and other appropriate entities to other potential victims. Systematic and routine risk assessments of information infrastructures provide a good starting point for effective risk management and thus should be a priority. An incident management plan should be developed and implemented with the approval of senior level decision makers and legal counsel. Law enforcement contact numbers should be readily available in case of an attack.

Follow Standard 'Best Practices' for Computer and Physical Security

Prevention of cyber attacks in the near future will be no different than in the past. Best practices for maintaining systems should be followed as a tenet of any organization's standard operating procedures:

- Operating systems and software should be updated regularly
- Strong password policies should be enforced
- Systems should be 'locked down'
- All unnecessary services should be disabled
- Anti-virus software should be installed and kept up to date
- High fidelity intrusion detection systems (IDS)[xxxi] and firewalls should be employed

Security measures, which were previously considered excessive, should now be considered a minimum effort. System administrators must recognize that this new war on terrorism will require increased vigilance from everyone, particularly those who are entrusted with maintaining critical information assets. These basic steps will go a long way toward preventing cyber attacks.

[xxxi] Intrusion Detection System: software program that attempts to detect intrusion into a computer or network by observation of actions, security logs, or audit data. (Footnote definitions compiled from three primary sources: cnet.com sans.org techtarget.com)

Secure Critical Information Assets

Any host or network component - the loss of whose services might result in serious communications failure or financial loss - should be considered a critical information asset. While cost considerations make extraordinary protection of all systems unfeasible, measures for securing critical systems should be implemented wherever possible. Anti-defacement measures include checks for characters associated with popular web server exploits. Border routers should make use of existing authentication mechanisms to prevent malicious tampering with routing tables. Domain name servers should be running only recent and secure software to prevent DNS corruption and the redirecting of web traffic to bogus sites. All vital data should be backed up regularly and stored off-site to prevent loss in the case of a physical or cyber attack.[37] Log records should also be copied and maintained in a secure location to avoid tampering. All the measures to secure critical infrastructure assets should be clearly explained in an enforceable security policy.

Ingress and Egress Filtering

Packets associated with cyber attacks, particularly DDoS attacks, are often 'spoofed'. This means that the real Internet protocol (IP) source address in the packet is replaced with a false address to disguise the identity of the attacker. Spoofed IP addresses are easy to detect and stop near their source, since routers can be programmed to discard any outbound packets whose source IP address does not belong to the router's client networks. Such outbound or 'egress' filtering is a relatively simple but not widely implemented validation procedure. Likewise, inbound or 'ingress' filtering of any IP packets with un-trusted source addresses, before they have a chance to enter the network, can also be effective.[38] Untrusted source addresses include those addresses reserved for private networks or not yet issued by the international authorities that assign Internet numbers. Filtering of packets from domains in hostile parts of the world might seem like a good way to minimize threats during a time of international strife, but IP address spoofing and attacks from within our own borders could circumvent such preventive measures. Countermeasures for DDoS can also include cooperation from 'upstream' Internet service providers (ISP's) that send packets to their client networks. ISP routers can be programmed to limit the rate at which packets typically associated with attacks (SYN and ICMP packets)[xxxii] are sent downstream to client networks. By rate limiting these particular packets, the effects of a malicious flood can be minimized without seriously disrupting normal operations. These preventive measures are well within the capabilities of most Internet service providers.

[xxxii] A SYN packet (used to 'sync up' or start computer communications) and Internet Control Message Protocol (ICMP) packets are often used in distributed denial of service DDoS attacks.

CONCLUSIONS

An examination of historical precedents indicates that major political and military conflicts are increasingly accompanied by significant cyber attack activity. Previous and ongoing global conflicts also indicate that cyber attacks are escalating in volume, sophistication, and coordination. The United States and its allies must operate under the premise that military strikes against terrorists and their nation-state supporters will result in cyber attacks against U.S. and allied information infrastructures.

The vast majority of previous politically related cyber attacks have been nuisance attacks, and it is extremely likely that such attacks will follow any U.S.-led military action. The factual data contained in this report suggests that the potential exists for much more devastating cyber attacks following any U.S.-led retaliation to the September 11 terrorist attacks on America. Such an attack could significantly debilitate U.S. and allied information networks. A catastrophic cyber attack could be launched either externally or internally on United States' information infrastructure networks and could be part of a larger conventional terrorist action.

APPENDIX: RELATED ONLINE RESOURCES

http://www.cert.org
The Carnegie Mellon Computer Emergency Response Team (CERT) Coordination Center is a major reporting center for Internet security problems that analyzes product vulnerabilities, publishes technical documents, and presents training courses.

http://www.fedcirc.gov/
The Federal Computer Incident Response Center (FedCIRC) is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government.

http://www.incidents.org
Incidents.org is a community and industry collaboration on security-related matters that produces practical technologies, tools, and processes that can be used by the entire Internet community to detect threats, protect their resources, and react to security incidents and new threats.

http://ists.dartmouth.edu
The Institute for Security Technology Studies at Dartmouth College serves as a principal national center for counterterrorism technology research, development, and assessment, with a significant focus on cyber attacks.

http://www.nipc.gov
The National Infrastructure Protection Center (NIPC) serves as the national focal point for threat assessment, warning, investigation, and response to cyber attacks. A significant part of its mission involves establishing mechanisms to increase the sharing of vulnerability and threat information between the government and private industry.

http://www.sans.org
The System Administration, Networking and Security (SANS) Institute is a cooperative research and education organization through which system administrators, security professionals, and network administrators share lessons learned. SANS provides system and security alerts, news updates, and education.

APPENDIX: INCIDENT REPORTING GUIDELINES

If you require immediate assistance for a computer security incident contact the appropriate law enforcement agency immediately and report the following:

- Names, location, and purpose of operating systems involved

- Names and location of programs accessed

- How intrusion access was obtained

- Highest classification of information stored in the systems

- Impact (compromise of information of dollar loss)

To protect evidence and help law enforcement agencies investigate the incident take the following actions:

- Make backup copies of damaged or altered files, and keep these backups in a secure location

- Activate all auditing software

- Consider implementing a keystroke monitoring program, provided an adequate warning banner is displayed on your system

- DO NOT contact the suspected perpetrator

Please address comments or questions to:

THE INSTITUTE FOR SECURITY TECHNOLOGY STUDIES

45 Lyme Road, Hanover, New Hampshire 03755, Telephone: 603-646-0700, FAX: 603-646-0660

http://www.ists.dartmouth.edu

Director

Michael A. Vatis

Research Staff for the Report

George Bakos
Marion Bates
Hanna Cerwall
Henry 'Chip' Cobb
Julie Cullen
Garry Davis
Todd DeBruin
Paul Gagnon
Trey Gannon
Eric Goetz
David Koconis, Ph.D.
Andrew Macpherson
Dennis McGrath
Susan McGrath, Ph.D.
William Stearns

PUBLICATION NOTICE

ENDNOTES

[1] We have already seen the early effects of this escalation in the time since the terror attacks in New York and Washington, with cyber attacks going in both directions. For example: (1) the web site of the Taliban mission to the U.N. was defaced twice in the days following the attacks. (2) A hacker by the name Fluffi Bunni redirected hundreds of web sites in the United Kingdom to a defaced site that ridiculed religion and American imperialism. (3) A group calling itself the Dispatchers issued a statement saying that more than 60 hackers would use their expertise to disable Arab and Islamic 'targets'. Anticipating an increase in cyber attacks, the NIPC issued a statement on September 14 calling for "increased cyber awareness" in the wake of the attacks. See NIPC advisory 01-021 "Potential Distributed Denial of Service(DDoS) Attacks" see: http://www.nipc.gov/warnings/advisories/2001/01-021.htm. The hacker group 'Chaos Computer Club' from Germany called for restraint following the terrorist attacks, but it is unlikely that all hackers will heed these calls.   Kettmann, Steve, "Venerable Hackers Urge Restraint", *Wired News*, September 15, 2001.

[2] "Pro-Pakistan Hackers Deface Centre's Venture Capital Site", *The Statesman*, August 21, 2001.

[3] Prasad, Ravi, Visvesvaraya, "Hack the Hackers", *The Hindustan Times,* December 19, 2000.

[4] Ghosh, Nirmal, "Indo-Pakistan Cyberwar a Battle in Earnest", *The Straits Times*. June 16, 2001.

[5] Cohen, Adam, "Schools For Hackers", *Time Magazine*, May 2, 2000.

[6] As of 21 May 2001, attrition.org ended its active mirroring of defaced web pages. As such, the data here is limited to the period shown.

[7] Lev, Ishtar, "E-Infitada: Political Disputes Cast Shadow in Cyberspace", *Jane's Intelligence Review,* December 1, 2000.

[8] Sale, Richard, "Mideast Conflict Roars into Cyberspace", *United Press International*, December 7, 2000.

[9] Messmer, Ellen, "Serb Supporters Sock it to NATO and U.S. Computers", *Network World*. April 5, 1999.

[10] Ibid.

[11] The Supreme Headquarters Allied Powers Europe website was defaced during the conflict, as were sites belonging to the U.S. Navy and commercial entities.

[12] Messmer, Ellen, Op. Cit.,

[13] NIPC Advisory (01-009). "Increased Internet Attacks Against U.S. Web Sites and Mail Servers Possible in Early May." April 26, 2001.

[14] For instance, according to Keith Rhodes, Chief Technologist at the General Accounting Office (GAO), the 'Code Red' worm, which is estimated to have caused $2.4 billion in damages, can be traced to a university in Guangdong, China. "Report: Code Red Computer Worm Born in China," Reuters, August 30, 2001. This is contradicted by other computer security experts who have been unable to ascertain the worm's origin.

[15] www.attrition.org

[16] "White House Website Attacked", *BBC News,* May 5, 2001.

[17] http://www.eeye.com/html/press/PR19990608.html

[18] http://www.cert.org/advisories/CA-2001-20.html

[19] http://www.fbi.gov/pressrel/pressrel01/nipc030801.htm

[20] Infowar, November 4, 1999

[21] Statement for the record by Michael A. Vatis, Director, National Infrastructure Protection Center (NIPC), Federal Bureau of Investigations (FBI), on NIPC Cyber Threat Assessment before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism, October 6, 1999.

[22] The State Department designates Iran, Iraq, Syria, Libya, Cuba, North Korea and Sudan as those seven states currently sponsoring international terrorism. "Patterns of Global Terrorism", Office of the Coordinator for Counterterrorism, U.S. Department of State. April 2001.

[23] Pakistan could potentially also become the target of U.S. and allied military strikes if it fails to cooperate in the campaign against terrorism, or if the present government is toppled by Islamic militants. Three people were killed in Karachi on September 21, 2001, during protests against the Pakistani government's announcement that it would assist the United States in its attempts to apprehend Osama bin Laden and his Al Qaeda organization. MacDonald, Scott and Khan, Ibrahim, "Three Killed in Pakistan as Anti-U.S. Demos Rage", Reuters. September 21, 2001.

[24] In fact, the most recent Defense Science Board report puts the number of states that already have, or are developing, computer attack capabilities at over 20. "Protecting the Homeland", Report of the Defense Science Board Task Force on Defensive Information Operations, March 2001.

[25] Ibid

[26] "Virtual Defense", *Foreign Affairs,* May 2001-June2001. "Cyber Security: Nations Prepare for Information Warfare", *National Journal's Technology Daily*, June 19, 2001.

[27] "America Widens 'Crusade' on Terror", *BBC News,* September 16, 2001.

[28] "Old friends, best friends – Solidarity from Europe", *The Economist*, September 15-21.

[29] A twenty-year-old hacker was able to gain access to Yahoo! News' systems and manipulate a story about Russian programmer Dimtry Sklyarov. The news story claimed that Mr. Sklyarov was now facing the death penalty for his violations of the Digital Millennium Copyright Act (DMCA). "Yahoo! News Hacked", *SecurityFocus*, September 21, 2001.

[30] See, Weaver Nicholas C. "Warhol Worms: The Potential for Very Fast Internet Plagues", University of California Berkeley, August 15, 2001 and Staniford Stuart, Gary Grim, Roelof Jonkma, "Flash Worms: Thirty Seconds to Infect the Internet", *Silicon Defense*, August 16, 2001.

[31] NIPC advisory "Increased Cyber Awareness" September 14, 2001.

[32] The Nimda worm is an example of a dangerous hybrid worm, although it remains unclear whether Nimda is politically motivated or has any link to the terrorist attacks of September 11, 2001.

[33] Statement for the Record of Ronald L. Dick, Director National Infrastructure Protection Center, Federal Bureau of Investigations on Critical Infrastructure Protection before the Senate Judiciary Committee, Subcommittee on Technology Terrorism and Government information, July 25, 2001 and "Cyber Threats and Information Security – Meeting the 21st Century Challenge", Center for Strategic and International Studies, December, 2000.

[34] Department of Defense news briefing see: http://www.defenselink.mil/news/Apr1998/t04161998_t0416asd.html

[35] "Hackers Stumble Upon California Power Grid", *News Bytes*, 12 June, 2001.

[36] Ibid.

[37] A number of criminal cases are reportedly in jeopardy after evidence, collected by the Bureau of Alcohol Tobacco and Firearms, the U.S. Customs Service, and the Secret Service, was lost in the terrorist attacks on the World Trade Center on September 11, 2001. There apparently were no copies of the evidence off site. "From Guns to Narcotics Evidence Lost in New York Threatens Case", *Wall Street Journal,* September 20, 2001.

[38] See RFC 2267 http://www.landfield.com/rfcs/rfc2267.html